7.1

Some arithmetic

Syllabus

Permutations and combinations;
Euclid's algorithm;
induction.

7.2

Choosing elements from a set

Suppose we have a set A of n elements $a_1, \ldots, a_n$,
and we have to choose k distinct elements of A in some order.

How many ways are there to do this?

7.3

For the first choice, call it b_1, we have n possibilities.
After b_1 is chosen, there are $n-1$ elements left in A,
so we have $n-1$ choices for the next element b_2.

So the number of ways of choosing an element b_1 and then another element b_2 is

$$n \times (n-1).$$

7.4

The same applies for choosing k elements in turn.
The number of ways of doing it is

$$\begin{aligned} & n \times (n-1) \times \ldots \times (n-(k-1)) \\ = \; & n \times (n-1) \times \ldots \times (n-k+1). \end{aligned}$$

We call this number $P(n,k)$.

7.5

$$\begin{aligned} P(n,k) &= n \times (n-1) \times \ldots \times (n-k+1) \\ &= \tfrac{n \times (n-1) \times \ldots \times (n-k+1) \times (n-k) \times \ldots \times 1}{(n-k) \times \ldots \times 1} \\ &= \tfrac{n!}{(n-k)!}. \end{aligned}$$

This gives us the important formula

$$P(n,k) = \frac{n!}{(n-k)!}.$$

7.6

The number $P(n,n)$ is the number of ways of arranging a set of n objects in order.
These ways are called the *permutations* of the set.
Remember that $P(n,n) = n!$.

7.7

Example. The set of all permutations of the set $\{a,b,c,d\}$ is

$$abcd, abdc, acbd, acdb, adbc, adcb, bacd, badc,$$
$$bcad, bcda, bdac, bdca, cabd, cadb, cbad, cbda,$$
$$cdab, cdba, dabc, dacb, dbac, dbca, dcab, dcba.$$

The number of permutations is $24 = 4!$.

7.8

Now we come back to $C(n,k)$, the number of ways of choosing k items from a set of n items.

$P(n,k)$ is the number of ways of choosing k items *in some order* from a set of n elements.

But this counts each set of chosen items $k!$ times, because k items can be arranged in $k!$ different orders.

So we get $C(n,k)$ by dividing $P(n,k)$ by $k!$:

$$C(n,k) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k)!}.$$

7.9

For example

$$\begin{aligned} C(5,5) &= \tfrac{5!}{5!\times 0!} = \tfrac{120}{120\times 1} = 1, \\ C(5,4) &= \tfrac{5!}{4!\times 1!} = \tfrac{120}{24\times 1} = 5, \\ C(5,3) &= \tfrac{5!}{3!\times 2!} = \tfrac{120}{6\times 2} = 10, \end{aligned}$$

agreeing with Pascal's triangle.

Since $C(n,k) = C(n,n-k)$, we've already calculated $C(5,2) = C(5,3) = 10$, $C(5,1) = C(5,4) = 5$ and $C(5,0) = C(5,5) = 1$.

7.10

Question: How many different strings can we get by rearranging the letters in the word HUBBUB?

Answer. We first answer a different question.
Suppose the word is $HU_1B_1B_2U_2B_3$, using labelled letters.
Then the number of permutations is $6!$,
since the word has six letters.

But . . .

7.11

But we've counted each combination of letters of HUBBUB six times too often, because we counted the $3!$ permutations of B, B, B as different;
and again twice too often, because we counted the $2!$ permutations of U, U separately.

So the answer is

$$\frac{6!}{3!\times 2!} = \frac{720}{6\times 2} = 60.$$

7.12

Question: What is the coefficient of x^2y^2zt in $(x+y+z+t)^6$?

Answer. There are six factors, and we have to find the number of ways of choosing x from two, y from two, and z and t from the two remaining factors.

There are $C(6,2)$ ways of choosing the factors to give x.

7.13

For each of these ways, there are $C(4,2)$ ways of choosing two of the remaining four factors to give y.
For each of these ways, there are $C(2,1)$ ways of choosing which of the two remaining factors gives z.
Then t comes from the remaining factor, and for this we have no choice.

7.14

So the number of ways in all is

$$\begin{aligned} & C(6,2) \times C(4,2) \times C(2,1) \\ = \ & \tfrac{6!}{2!\times 4!} \times \tfrac{4!}{2!\times 2!} \times \tfrac{2!}{1!\times 1!} \\ = \ & 15 \times 6 \times 2 \\ = \ & 180. \end{aligned}$$

7.15

Same question: What is the coefficient of x^2y^2zt in $(x+y+z+t)^6$?

Second answer. The answer is the number of rearrangements of the word $xxyyzt$.
By our previous method, this is

$$\frac{6!}{2! \times 2!} \ = \ 6 \times 5 \times 3 \times 2 \ = \ 180$$

as before. Both methods have their advantages.

7.16

Properties of division

We shall study the set $\mathbb{Z}$ of integers

$$\ldots, -2, \ -1, \ 0, \ 1, \ 2, \ldots$$

7.17

Division Lemma: Let m be a positive integer and n any integer. Then there are unique integers q and r such that

- $n = qm + r$,
- $0 \leqslant r < m$.

q is called the *quotient* and r is called the *remainder* (when n is divided by m).

7.18

The equation $n = qm + r$ can also be written

$$\frac{n}{m} = q + \frac{r}{m}.$$

This tells us how to find q and r:

Divide n by m.
The integer part of the answer is q, and the remainder is r.

7.19

Examples with $m = 8$:

- $4 = 0 \times 8 + 4$.
- $13 = 1 \times 8 + 5$.
- $50 = 6 \times 8 + 2$.
- $-5 = (-1) \times 8 + 3$.

7.20

When $n = qm$ for some integer q,
in other words
when the remainder after dividing n by m is 0,
then we say that m *divides* n.

The symbol for 'm divides n' is $m|n$.
But we won't use it much, because it's very easy to confuse the statement $m|n$ with the number m/n.

7.21

Facts about dividing

If m divides a and m divides b,
then m divides $a + b$ and $a - b$.

If m divides a and x is an integer, then m divides xa.

Every integer divides 0.

1 divides every integer.

7.22

Euclid's Algorithm

The ancient Greek mathematician Euclid suggested
using the division lemma over and over again
until the remainder is zero, as follows.

In this example we start with $n = 165$, $m = 49$.

7.23

$$165 = 3 \times 49 + 18$$

$$49 = 2 \times 18 + 13$$

$$18 = 1 \times 13 + 5$$

$$13 = 2 \times 5 + 3$$

$$5 = 1 \times 3 + 2$$

$$3 = 1 \times 2 + \mathbf{1}$$

$$2 = 2 \times 1 + 0$$

7.24

The important number is the *last nonzero remainder*,
in this case 1.

We can use the equations to write this remainder
in terms of the first two numbers, 165 and 49,
to get an equation of the form

$$1 = 165a + 49b,$$

as follows.

7.25

$$\begin{aligned}
1 &= 3 - 1 \times 2 \\
&= 3 - 1(5 - 1 \times 3) && = 2 \times 3 - 5 \\
&= 2 \times (13 - 2 \times 5) - 5 && = 2 \times 13 - 5 \times 5 \\
&= 2 \times 13 - 5 \times (18 - 1 \times 13) && = 7 \times 13 - 5 \times 18 \\
&= 7 \times (49 - 2 \times 18) - 5 \times 18 && = 7 \times 49 - 19 \times 18 \\
&= 7 \times 49 - 19 \times (165 - 3 \times 49) && = 64 \times 49 - 19 \times 165.
\end{aligned}$$

7.26

So we get

$$1 \;=\; 64 \times 49 - 19 \times 165 \;=\; 3136 - 3135.$$

By the facts about division, this equation shows that
every integer that divides 165 and 49 must also divide 1.
In other words, the only integers that divide both 165 and 49 are 1 and -1.
We express this by saying 165 and 49 are *relatively prime*.

7.27

Suppose we apply Euclid's algorithm to integers m and n.
Let d be the last nonzero remainder.
Then the algorithm finds integers a, b so that

$$d = an + bm.$$

So any integer that divides both m and n also divides d.

7.28

But also we can see, starting off from the bottom equation and working upwards, that d divides all the remainders and divides n and m.

We call d the *greatest common divisor* of n and m, sometimes written GCD(n, m).

An integer divides both n and m if and only if it divides d.

7.29

Example from Exam 2003:

Use Euclid's algorithm to find the greatest common divisor d, say, of 6648 and 1032 and find integers u, v such that $d = 6648u + 1032v$.

7.30

SOLUTION.

$$\begin{aligned} 6648 &= 6 \times 1032 + 456. \\ 1032 &= 2 \times 456 + 120. \\ 456 &= 3 \times 120 + 96. \\ 120 &= 1 \times 96 + 24. \\ 96 &= 4 \times 24. \end{aligned}$$

7.31

So $d = 24$ and

$$\begin{aligned} 24 &= 120 - 1 \times 96 \\ &= 120 - 1 \times (456 - 3 \times 120) &&= 4 \times 120 - 1 \times 456 \\ &= 4 \times (1032 - 2 \times 456) - 1 \times 456 &&= 4 \times 1032 - 9 \times 456 \\ &= 4 \times 1032 - 9 \times (6648 - 6 \times 1032) &&= 58 \times 1032 - 9 \times 6648. \end{aligned}$$

So putting $u = -9$ and $v = 58$, we have

$$24 = d = 6648u + 1032v.$$